



FortiGate Connector for Cisco ACI - Release Notes

Version 1.2

FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO GUIDE

<http://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

<http://cookbook.fortinet.com/how-to-work-with-fortinet-support/>

FORTIGATE COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING SERVICES

<http://www.fortinet.com/training>

FORTIGUARD CENTER

<http://www.fortiguard.com>

END USER LICENSE AGREEMENT

<http://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdocs@fortinet.com



Thursday, May 19, 2016

Release Notes- FortiGate Connector for Cisco ACI v1.2

01-540-371310-20160505

FortiGate Connector for Cisco ACI v.1.1

Introduction

This document provides the following information for FortiGate Connector v1.2 for Cisco ACI v1.2 (2.x). This product can also refer as FortiGate Device Package for Cisco APIC.

- [Special Notices](#)
- [Product Integration and Support](#)
- [Known Issues](#)
- [Limitations](#)

Supported Models

FortiGate Connector for Cisco ACI v1.2 supports the following predefined models:

- FG-600D
- FG-900D
- FG-1000D
- FG-1200D
- FG-1500D
- FG-3000D
- FG-3100D
- FG-3200D
- FG-3700D
- FG-VM

Unknown models

The use of FortiGate Connector can be attempted with any FortiGate model, but do so with caution. Only those listed above have been confirmed. If an unknown model of FortiGate is used, the user needs to verify port names match the real FortiGate model.

Supported Features

The FortiGate Connector for Cisco ACI supports the following functions:

Baseline features from v.1.0 to v.1.1

- Cisco ACI service insertion - software package for FortiGate device deployed to Cisco APIC, containing FortiGate models, function description, version, credentials, as a L4-L7 service.
- Enable tenant configuration to add/modify/delete L4-L7 device of FortiGate firewall service.
- Enable FortiGate deployment as both physical and virtual device (FortiGate chassis & VM).
- Support both transparent (GoThrough) and L3 (GoTo) device mode .
- Automatically create VDOM (context). One VDOM per logical device under a tenant.
- Enable FortiGate specific interface configuration: physical interface and port channel.
- Support IP address configuration on Layer 3 interfaces.
- Support subnet and service object configuration.
- Enable FortiGate firewall device to connect to endpoint groups (EPGs).
- Support IPv4 policies: match, action, network operations & security features' selection.
- Support NAT.
- Enable service graph to add/modify/delete FortiGate firewall service node
- Multiple interfaces can be added in the same device
- Single logical port can be shared in the same EPG for multiple service graphs
- Single VDOM can be used in multiple service graphs

Additional features added in v1.2

- High Availability (Active-Standby Mode)
- OSPF based routing configuration in the L3 (GoTo) mode
- Support for logging and error reporting of Fortigate as a L4-L7 device
- Automatically create VDOM based on APIC virtual device ID
- Policy enable/disable support
- Enable/Disable DDoS features
- Enable/Disable UTM Security Profiles

Special Notices

Predefined keywords

Do not modify the predefined key words used by FortiGate.

Custom Addresses and Services character limitations

The name fields of Firewall Addresses and Services should not include spaces or special characters.

VDOM name limitations

Beginning with FortiGate Connector v1.2, VDOM name is no longer a configurable option due to design recommendation from Cisco. The VDOM name will be the virtual device ID. After a service graph is deployed, a virtual Device ID is randomly assigned by Cisco APIC and that will be the VDOM name appears on Fortigate.

Rule ID sequence and Policy Name

Rule ID with lowest number will get processed and listed first on the FortiGate. In addition, if deploying multiple service graphs shared with same virtual device, please ensure Rule IDs and Policy Names are unique otherwise, they will override each other.

OSPF Configuration

User doesn't need to perform any OSPF parameter configuration except Router ID configured in Router Configurations under L4-L7 services. The recommendation from Cisco is that user creates OSPF Configuration on L3OUTs which is the corresponding interface configuration along with all OSPF parameters to the FortiGate on APIC. During the Service Graph deployment, Fortigate Connector device package will extract the OSPF parameters from APIC and then program the corresponding OSPF configurations on FortiGate.

Transparent Mode and NAT Mode Configuration

Beginning with FortiGate FortiConnector v1.2, the device package no longer has the option to select VDOM mode. When Go-Through mode is selected, interface ip address field must be in default setting; when "GoTo" mode is selected, interface ip addresses must be configured with valid ip address and network mask.

Change of VRF mapping After Service Graph Deployed

We uncovered a design issue for specific scenario where user changed VRF mapping after the service graph deployed which caused out of sync behavior between Cisco APIC and FortiGate.

We are actively working with Cisco to address this issue. At the meantime, the work around will be to remove the service graph, change the VRF mapping and then re-deploy the service graph. This behavior was observed on APIC version 1.2(3c) but not in 1.3(1g).

Static Route Sequence Number

For Static Route Sequence Number of 0 (default value), Device Package will ignore static route programming. Otherwise, Device Package will program any entry in the Static Route fields when Sequence Number is greater than 0.

Product Integration and Support

Fortinet Products

This Version of FortiConnector for Cisco ACI is compatible with the following firmware:

- FortiOS 5.4.0 and above

Cisco Environment

This Version of FortiConnector for Cisco ACI is supported by the following Cisco ACI environments:

- Cisco ACI v1.2 (2.x) or above

Known Issues

The following issues have been identified in version 1.2. For inquiries about a particular bug or to report a bug, please contact Customer Service & Support.

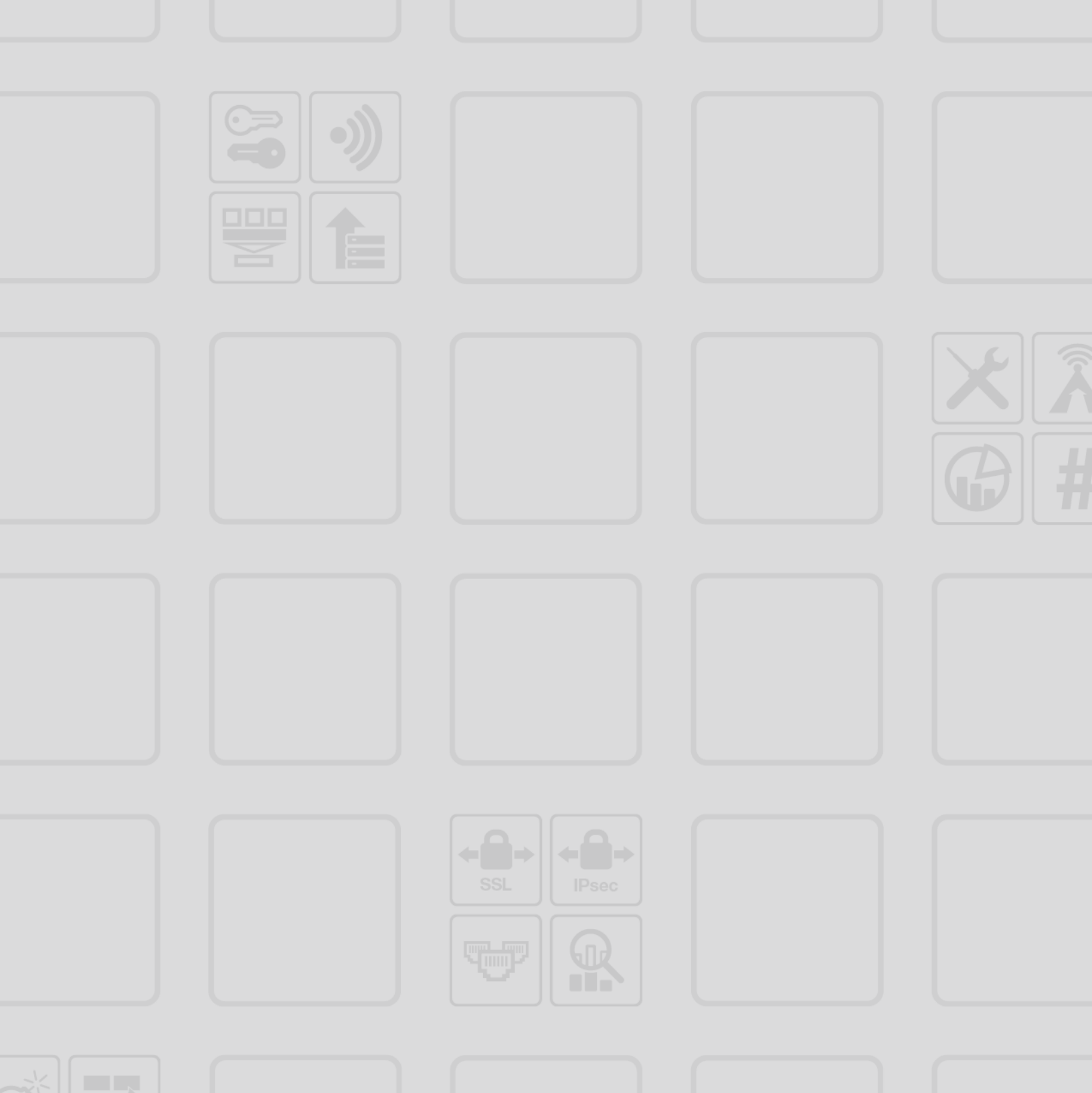
Bug ID	Description
0308841	REST API via Cisco APIC to push multiple VDOMs creation observe crash on FortiGate
0306906	VDOM creation task takes a long time when there are already an extensive number of VDOMs configured on the FortiGate

Known issues from previous versions not listed here have been resolved.

Limitations

There are limitations to the FortiGate Connector and FortiGate combination. Some of these will be limitations of what the FortiGates can do in the environment. Some of these limitations will be what the FortiGate Connector can do. The limitations are:

- Dynamical routing protocol BGP is not supported.
- DNAT and other FortiGate features are not supported. But, user can manually configure them on FortiGate after Service Graph is deployed.



FORTINET®

High Performance Network Security



Copyright© 2016 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.